Power integral bases in prime-power cyclotomic fields

István Gaál*
Mathematical Institute
University of Debrecen
H-4010 Debrecen Pf. 12, Hungary
E-mail: igaal@math.klte.hu

Leanne Robertson
Department of Mathematics
Smith College
Northampton, MA 01063, U.S.A.
E-mail: lroberts@math.smith.edu

January 21, 2005

Abstract

Let p be an odd prime and $q = p^m$, where m is a positive integer. Let ζ be a primitive qth root of unity, and $\mathcal{O}_q$ be the ring of integers in the cyclotomic field $\mathbb{Q}(\zeta)$. We prove that if $\mathcal{O}_q = \mathbb{Z}[\alpha]$ and $\gcd(h_q^+, p(p-1)/2) = 1$, where h_q^+ is the class number of $\mathbb{Q}(\zeta + \zeta^{-1})$, then an integer translate of α lies on the unit circle or the line $\mathrm{Re}(z) = 1/2$ in the complex plane. Both are possible since $\mathcal{O}_q = \mathbb{Z}[\alpha]$ if $\alpha = \zeta$ or $\alpha = 1/(1+\zeta)$. We conjecture that, up to integer translation, these two elements and their Galois conjugates are the only generators for $\mathcal{O}_q$, and prove that this is indeed the case when $q = 25$.

1 Introduction

A number field K is said to have a *power integral basis* if its ring of integers is of the form $\mathbb{Z}[\alpha]$ for some $\alpha \in K$. It is a well-known problem to determine if a number field has a power integral basis, and, if it does, to find all the elements that generate such a basis. Interest in this problem goes back at least as far as Dedekind [**?**], who provided the first example of a number field that does not have a power integral basis. For a general survey of the topic see Győry [**?**]. It is rare for a number field to have a power integral basis and when one does exist it is usually very difficult to determine all the

*Research supported in part by Grants T 037367 and T 042985 from the Hungarian National Foundation for Scientific Research.

generators. See Gaál [**?**] for known results on the existence and computation of power integral bases, and for algorithms for determining them.

Cyclotomic fields are an interesting case because power integral bases always exist and in some cases we can find all the generators. See Bremner [**?**] and Robertson [**?**] for a study of power integral bases in prime cyclotomic fields. See Robertson [**?**] for the determination of all power integral bases in 2-power cyclotomic fields. In this paper we study power integral bases in p-power cyclotomic fields for odd primes p.

Let p be an odd prime, $q = p^m$, ζ be a primitive qth root of unity, and $\mathcal{O}_q$ be the ring of integers of the cyclotomic field $\mathbb{Q}(\zeta)$. It is well known that $\mathcal{O}_q = \mathbb{Z}[\zeta]$, so ζ generates a power integral basis. The set of generators is stable under integer translation, Galois conjugation, and multiplication by -1; we call α and α' *equivalent* if $\alpha' = n \pm \sigma(\alpha)$ for some $n \in \mathbb{Z}$, $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Győry [**?**] proved that up to equivalence there are only finitely many elements that generate a power integral basis for any number field K. Thus, up to equivalence, there are only finitely many elements α such that $\mathbb{Z}[\alpha] = \mathbb{Z}[\zeta]$ and we would like to determine them all.

In the case where ζ is a pth root of unity it was shown in Robertson [**?**] that if $\mathbb{Z}[\alpha] = \mathbb{Z}[\zeta]$ and α is not equivalent to ζ, then $\alpha + \bar{\alpha}$ is an odd integer, where the "bar" denotes complex conjugation. Since we are only interested in determining the generators of $\mathbb{Z}[\zeta]$ up to integer translation, it is sufficient to find those on the unit circle and on the line $\mathrm{Re}(z) = 1/2$ in the complex plane. This significantly reduced the computations when determining all power integral bases for specific values of p. In Theorem **??** (proven in Section 3) we generalize this result to the case where ζ is a p^mth root of unity, $m > 1$. This theorem reduces the number of indeterminants defining α from $\phi(q) = (p-1)p^{m-1}$ to $\phi(q)/2$, where ϕ is the Euler phi function. Our proof in the p-power case requires an additional class number condition.

Theorem 1.1 *Let p be an odd prime, $q = p^m$, and ζ be a primitive qth root of unity. Let h_q^+ denote the class number of the maximal totally real subfield $\mathbb{Q}(\zeta + \zeta^{-1})$ of the cyclotomic field $\mathbb{Q}(\zeta)$. If $\mathbb{Z}[\alpha] = \mathbb{Z}[\zeta]$ and $\gcd(h_q^+, p(p-1)/2) = 1$, then either α is equivalent to ζ or $\alpha + \bar{\alpha}$ is an odd integer.*

Van der Linden [**?**] has shown that $h_q^+ = 1$ if $\phi(q) \leq 66$, and if we assume the generalized Riemann hypothesis then $h_q^+ = 1$ if $\phi(q) < 162$. The following is thus a corollary of Theorem **??** and the result in [**?**] for prime cyclotomic fields mentioned above.

Corollary 1.2 *Let ζ be a primitive qth root of unity. Suppose q is prime or $q = 3^2, 3^3, 3^4, 5^2, 7^2$. If $\mathbb{Z}[\alpha] = \mathbb{Z}[\zeta]$ and α is not equivalent to ζ, then $\alpha + \bar{\alpha}$*

is equal to an odd integer. If we assume the generalized Riemann hypothesis, then in addition the result holds for $q = 5^3, 11^2, 13^2$.

Although the value of h_q^+ is not known for a single value of q with $\phi(q) > 66$, conjectures and heuristics suggest that for a given q it is very likely that $\gcd(h_q^+, p(p-1)/2) = 1$. Indeed, the Kummer-Vandiver conjecture that h_p^+ is not divisible by p implies that h_q^+ is not divisible by p for all m [**?**, Corollary 10.5]. The Kummer-Vandiver conjecture has been verified for all p less that 12 million [**?**], so $\gcd(h_q^+, p) = 1$ for all $p < 12000000$ and $m \geq 1$. Also, in the prime case, Schoof [**?**] has a table of divisors of the class numbers h_p^+ for the 1228 odd primes p less than 10000, and argues on the basis of the Cohen-Lenstra heuristics on class groups that the probability that the table is actually a table of the class numbers h_p^+ is at least 98%. The table suggests that for a given p it is very likely that $\gcd(h_p^+, (p-1)/2) = 1$, although $\gcd(h_p^+, (p-1)/2) \neq 1$ for some primes p. Moreover, speculative extensions of the Cohen-Lenstra heuristics imply that for all but finitely many primes p, $h_q^+ = h_p^+$ for all positive integers m [**?**]. Thus, for a given q it seems likely that $\gcd(h_q^+, p(p-1)/2) = 1$, and the hypotheses of Theorem **??** are satisfied.

In the case of 2-power cyclotomic fields, there are no generators on the line $\mathrm{Re}(z) = 1/2$ in the complex plane and, up to equivalence, all the generators lie on the unit circle [**?**]. In the current case of p-power cyclotomic fields where p is an odd prime, there do exist generators for $\mathcal{O}_q$ that lie on the line $\mathrm{Re}(z) = 1/2$. Consider $\omega = 1/(1+\zeta)$. One easily checks that $\omega + \bar{\omega} = 1$, so $\mathrm{Re}(\omega) = 1$. Also, $1 + \zeta$ is a unit in $\mathbb{Z}[\zeta]$, so ω is an algebraic integer that is a unit in $\mathbb{Z}[\zeta]$.

Proposition 1.3 *Let* $\omega = 1/(1+\zeta)$. *Then* $\mathbb{Z}[\omega] = \mathbb{Z}[\zeta]$.

Proof. The inclusion $\mathbb{Z}[\omega] \subseteq \mathbb{Z}[\zeta]$ is immediate since $1 + \zeta$ is a unit in $\mathbb{Z}[\zeta]$. For the reverse inclusion, we use that the constant term of the minimal polynomial of ω is equal to ± 1 since ω is a unit. Thus, there are $a_i \in \mathbb{Z}$ such that $1 + a_1\omega + a_2\omega^2 + \cdots + a_{p-1}\omega^{p-1} = 0$. Multiplication by $1 + \zeta$ yields $1 + \zeta = -(a_1 + a_2\omega + a_3\omega^2 + \cdots + a_{p-1}\omega^{p-2})$, and $\zeta \in \mathbb{Z}[\omega]$. □

If $q > 3$ then it is clear that ω is not equivalent to ζ. Thus, up to equivalence there are at least two generators for $\mathcal{O}_q$, namely ζ and ω. When $q = 9$, Gaál and Pohst [**?**] proved that up to equivalence there are no additional generators for the ring of integers (the discriminant is -19683 and the nine generators listed for this discriminant correspond to the six conjugates of ζ and half of the conjugates of ω, since $\sigma_a(\omega)$ is equivalent to

$\sigma_a(\overline{\omega}) = \sigma_{9-a}(\omega)$). It is plausible that there are no additional generators for any prime-power q.

Conjecture 1.4 *If $\mathcal{O}_q = \mathbb{Z}[\zeta]$ then α is equivalent to ζ or ω.*

This conjecture is due to Bremner [**?**] in the case $m = 1$, and he proves the conjecture for $q = 7$. Bremner's conjecture has been verified for $p \leq 23$ [**?**, **?**]. Here we study power integral bases and Conjecture **??** in the case $m > 1$. As noted above, the conjecture holds when $q = 9$. In Section 4 we use Theorem **??** to prove the conjecture for $q = 25$.

2 Cyclotomic Units

Our work on power integral bases involves the study of units in $\mathbb{Z}[\zeta + \zeta^{-1}]$. In this section we prove two theorems involving cyclotomic units that are needed later.

We begin by establishing the notation that is used throughout this paper. As above, let p be an odd prime, $q = p^m$, and ζ be a primitive qth root of unity. Denote the elements of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ by σ_i, where $\sigma_i(\zeta) = \zeta^i$ and $1 \leq i \leq q$, $p \nmid i$. Denote the complex conjugate of $\alpha \in \mathbb{Q}(\zeta)$ by $\overline{\alpha}$. Let g be a primitive root modulo q. Then $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is cyclic of order $\phi(q) = (p-1)p^{m-1}$ and is generated by σ_g. Also, $\mathrm{Gal}(\mathbb{Q}(\zeta + \zeta^{-1})/\mathbb{Q})$ is cyclic of order $\phi(q)/2$ and is generated by σ_g.

The unit group of $\mathbb{Z}[\zeta + \zeta^{-1}]$ has rank r, where

$$r = \phi(q)/2 - 1 = (p-1)p^{m-1}/2 - 1.$$

In general it is difficult to find a fundamental system of r units. It is well known, however, that the unit group has a subgroup of finite index, namely the group of cyclotomic units, that can be given explicitly. Moreover, the index is equal to the class number h_q^+ of $\mathbb{Q}(\zeta+\zeta^{-1})$. Following Washington [**?**], let

$$\xi_a = \zeta^{(1-a)/2}\,\frac{1-\zeta^a}{1-\zeta},\ 1 < a < q,\ p \nmid a, \tag{1}$$

where the exponent $(1-a)/2$ is taken modulo q. These elements are cyclotomic units in $\mathbb{Z}[\zeta + \zeta^{-1}]$ and satisfy $\xi_{-a} = -\xi_a$. The group of cyclotomic units of $\mathbb{Z}[\zeta + \zeta^{-1}]$ is generated by -1 and the r distinct units

$$\xi_{g^i},\ 1 \leq i \leq r. \tag{2}$$

The cyclotomic units of $\mathbb{Z}[\zeta]$ are generated by ζ and the cyclotomic units of $\mathbb{Z}[\zeta+\zeta^{-1}]$.

The group of cyclotomic units of $\mathbb{Z}[\zeta+\zeta^{-1}]$ is closed under Galois conjugation. In particular,

$$\sigma_g\left(\xi_{g^i}\right) = \zeta^{(g-g^{i+1})/2} \cdot \frac{1-\zeta^{g^{i+1}}}{1-\zeta^g} = \begin{cases} \xi_g^{-1}\xi_{g^{i+1}} & \text{if } 1 \le i < r, \\ -\xi_g^{-1} & \text{if } i = r. \end{cases} \tag{3}$$

We will use this in our proof of Theorem **??**.

If $\tau \in \mathbb{Z}[\zeta+\zeta^{-1}]$ is a unit of norm 1, then it follows from Hilbert's Theorem 90 that $\tau = \sigma_g(\mu)/\mu$ for some unit $\mu \in \mathbb{Z}[\zeta+\zeta^{-1}]$. In Robertson [**?**] we considered the case where ζ is a primitive 2^mth root of unity and showed that if τ is a cyclotomic unit then μ is a cyclotomic unit as well. In the current case ζ is a primitive p^mth root of unity and we require the additional condition that $\gcd(h_q^+, p(p-1)/2) = 1$.

Theorem 2.1 *Let τ and μ be units in $\mathbb{Z}[\zeta+\zeta^{-1}]$ that satisfy $\tau = \sigma_g(\mu)/\mu$. If τ is a cyclotomic unit and $\gcd(h_q^+, p(p-1)/2) = 1$, then μ is a cyclotomic unit as well.*

Proof. The proof follows the proof in the 2-power case given in Robertson [**?**]. Let σ_g repeatedly act on the equation $\sigma_g(\mu) = \mu\tau$. This gives

$$\begin{array}{rcl} \sigma_g(\mu) &=& \mu\cdot\tau \\ \sigma_{g^2}(\mu) &=& \mu\cdot\tau\cdot\sigma_g(\tau) \\ \sigma_{g^3}(\mu) &=& \mu\cdot\tau\cdot\sigma_g(\tau)\cdot\sigma_{g^2}(\tau) \\ \sigma_{g^4}(\mu) &=& \mu\cdot\tau\cdot\sigma_g(\tau)\cdot\sigma_{g^2}(\tau)\cdot\sigma_{g^3}(\tau) \\ \vdots && \vdots \\ \mu \;=\; \sigma_{g^{r+1}}(\mu) &=& \mu\cdot\tau\cdot\sigma_g(\tau)\cdot\sigma_{g^2}(\tau)\cdot\sigma_{g^3}(\tau)\cdots\sigma_{g^r}(\tau). \end{array} \tag{4}$$

Now, μ has norm ± 1 since it is a unit. Since $\mathrm{Gal}(\mathbb{Q}(\zeta+\zeta^{-1})/\mathbb{Q})$ is cyclic of order $r+1$ and is generated by σ_g, multiplying the equations in (**??**) together yields

$$\pm 1 = \mathrm{Norm}_{\mathbb{Q}(\zeta+\zeta^{-1})/\mathbb{Q}}(\mu) = \prod_{i=1}^{\phi(q)/2} \sigma_{g^i}(\mu) = \mu^{(p-1)p^{m-1}/2}\cdot\gamma,$$

where γ is a cyclotomic unit since τ and all of its Galois conjugates are cyclotomic units. Therefore, $\mu^{(p-1)p^{m-1}/2} = \pm\gamma^{-1}$ is a cyclotomic unit as well. If $\gcd(h_q^+, p(p-1)/2) = 1$, then it follows that μ is a cyclotomic unit

since the index of the cyclotomic units in the full unit group of $\mathbb{Z}[\zeta + \zeta^{-1}]$ is equal to h_q^+. $\square$

The following theorem uses Theorem **??** and plays a central role in our work in the next section.

Theorem 2.2 *Let $\alpha \in \mathbb{Z}[\zeta]$. Suppose $\mu = \dfrac{\alpha - \overline{\alpha}}{\zeta - \overline{\zeta}}$ is a unit in $\mathbb{Z}[\zeta + \zeta^{-1}]$ and that there is an automorphism $\sigma_k \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ with*

$$\mu = \frac{\alpha - \overline{\alpha}}{\zeta - \overline{\zeta}} = \frac{\alpha - \sigma_g(\alpha)}{\zeta - \sigma_k(\zeta)}. \tag{5}$$

If $\gcd(h_q^+, p(p-1)/2) = 1$, then $\mu = \pm 1$ and $\alpha = n \pm \zeta$ for some $n \in \mathbb{Z}$.

Proof. The outline of the proof is as follows. We first show that

$$\mu = \sigma_g(\mu) \cdot \epsilon, \quad \text{where } \epsilon = \frac{\zeta^g - \zeta^{-g}}{\zeta^k - \zeta^{-k}}. \tag{6}$$

Note that $\epsilon = \xi_{2g}\xi_{2k}^{-1}$, and so ϵ is a cyclotomic unit. It follows from Theorem **??** that μ is a cyclotomic unit as well. This is the key fact in the proof. We write μ as a product of the generators for the group of cyclotomic units given in (**??**) and, using that $\mu = \sigma_g(\mu) \cdot \epsilon$, prove that $k \equiv \pm g \bmod q$ and so $\epsilon = \pm 1$. To finish the proof, we consider $\epsilon = -1$ and $\epsilon = 1$ separately.

To prove (**??**) we rewrite equation (**??**) as

$$\alpha - \mu\zeta = \sigma_g(\alpha) - \mu\zeta^k.$$

Since $\mu \in \mathbb{R}$, letting complex conjugation act on both sides of this equation gives

$$\overline{\alpha} - \mu\zeta^{-1} = \sigma_g(\overline{\alpha}) - \mu\zeta^{-k}.$$

But, $\alpha - \mu\zeta = \overline{\alpha} - \mu\zeta^{-1}$ by the definition of μ. Therefore we have

$$\sigma_g(\alpha) - \mu\zeta^k = \sigma_g(\overline{\alpha}) - \mu\zeta^{-k}.$$

Solving for μ yields

$$\mu = \frac{\sigma_g(\alpha) - \sigma_g(\overline{\alpha})}{\zeta^k - \zeta^{-k}} = \sigma_g\left(\frac{\alpha - \overline{\alpha}}{\zeta - \zeta^{-1}}\right) \cdot \frac{\zeta^g - \zeta^{-g}}{\zeta^k - \zeta^{-k}} = \sigma_g(\mu) \cdot \epsilon,$$

as claimed in (**??**). Therefore, as noted above, μ is a cyclotomic unit.

We next show that $k \equiv \pm g \bmod q$. Suppose, for a contradiction, that $k \not\equiv \pm g \bmod q$. Take the generators for the cyclotomic units to be as in (**??**). Then since $\xi_{-a} = -\xi_a$ we have

$$\mu = \sigma_g(u)\xi_{2g}\xi_{2k}^{-1} = \pm\sigma_g(u)\xi_{g^b}\xi_{g^c}^{-1}, \tag{7}$$

for some $1 \leq b, c \leq r$ with $b \neq c$ since $k \not\equiv \pm g \bmod q$ by assumption. Also, since μ is a cyclotomic unit there are unique integers n_i, $1 \leq i \leq r$ such that

$$\mu = \pm \prod_{i=1}^{r} \xi_{g^i}^{n_i}. \tag{8}$$

Using the conjugation formulas in (**??**), we may rewrite (**??**) as

$$u = \pm \prod_{i=1}^{r} \xi_{g^i}^{n_i} = \pm\xi_{g^b}\xi_{g^c}^{-1}\xi_g^{-N} \prod_{i=2}^{r} \xi_{g^i}^{n_{i-1}}, \tag{9}$$

where $N = \sum_{i=1}^{r} n_i$.

For each i, $1 \leq i \leq r$, the exponent of ξ_{g^i} on the left-hand side of (**??**) must be the same as the exponent of ξ_{g^i} on the right-hand side of (**??**), by the uniqueness of the exponents in (**??**). Comparing exponents gives

$$\begin{array}{rcccl} n_1 & = & -N + \delta_1 & & \\ n_2 & = & n_1 + \delta_2 & = & -N + \delta_1 + \delta_2 \\ n_3 & = & n_2 + \delta_3 & = & -N + \delta_1 + \delta_2 + \delta_3 \\ n_4 & = & n_3 + \delta_4 & = & -N + \delta_1 + \delta_2 + \delta_3 + \delta_4 \\ & \vdots & & \vdots & \\ n_r & = & n_{r-1} + \delta_r & = & -N + \delta_1 + \delta_2 + \delta_3 + \delta_4 + \cdots + \delta_r, \end{array} \tag{10}$$

where

$$\delta_i = \begin{cases} 1 & \text{if } i = b \\ -1 & \text{if } i = c \\ 0 & \text{otherwise.} \end{cases}$$

Adding the equations in (**??**) together

$$N = -rN + \sum_{i=1}^{r} (r + 1 - i)\delta_i.$$

Thus,

$$\begin{array}{rcl} (r+1)\,N & = & \displaystyle\sum_{i=1}^{r} (r + 1 - i)\delta_i \\ & = & (r + 1 - b) - (r + 1 - c) \\ & = & c - b \end{array}$$

This contradicts $N \in \mathbb{Z}$ since the absolute value of $c - b$ is less than $r - 1$ and is nonzero. Hence $k \equiv \pm g \bmod q$ as claimed. Therefore $\epsilon = \pm 1$.

Suppose $\epsilon = -1$ and $\mu = -\sigma_g(\mu)$. Then $\mu = -\sigma_g(-\sigma_g(\mu)) = \sigma_{g^2}(\mu)$ and μ is fixed by σ_{g^2}. The fixed field of σ_{g^2} is $\mathbb{Q}(\sqrt{\pm p})$, where we have $+$ if $p \equiv 1 \bmod 4$ and $-$ if $p \equiv 3 \bmod 4$, since the automorphism group generated by σ_{g^2} has index 2 in $\mathrm{Gal}(\mathbb{Q}(\zeta+\zeta^{-1})/\mathbb{Q})$ and $\mathbb{Q}(\sqrt{\pm p})$ is the unique quadratic subfield of $\mathbb{Q}(\zeta + \zeta^{-1})$. Thus, $\mu = a + b\sqrt{\pm p}$ and $\sigma_g(\mu) = a - b\sqrt{\pm p}$, for some $a, b \in \mathbb{Z}$. Now, $\mu = -\sigma_g(\mu)$ implies $a = 0$. This is a contradiction since $\mu = b\sqrt{\pm p}$ is not a unit.

Therefore $\epsilon = 1$ and $\mu = \sigma_g(\mu)$. Since σ_g generates $\mathrm{Gal}(\mathbb{Q}(\zeta + \zeta^{-1})/\mathbb{Q})$ if follows that μ is fixed by the entire Galois group and so $\mu \in \mathbb{Z}$. Hence $\mu = \pm 1$, as claimed in the statement of the theorem.

To finish the proof of Theorem **??**, it remains to show that $\alpha = n \pm \zeta$ for some $n \in \mathbb{Z}$. Well, $\epsilon = 1$ implies $k \equiv g \bmod q$ and so equation (**??**) may be rewritten as $\alpha - \mu\zeta = \sigma_g(\alpha - \mu\zeta)$. Thus $\alpha - \mu\zeta$ is fixed by σ_g and so $\alpha - \mu\zeta \in \mathbb{Z}$. Since $\mu = \pm 1$, this gives that $\alpha = n \pm \zeta$ for some $n \in \mathbb{Z}$. $\square$

3 Proof of Theorem 1.1

In this section we prove Theorem **??**. If $\mathbb{Z}[\alpha] = \mathbb{Z}[\zeta]$ then $(\alpha - \bar{\alpha})/(\zeta - \bar{\zeta})$ is a unit in $\mathbb{Z}[\zeta + \zeta^{-1}]$ by Lemma **??**. Our proof of Theorem **??** requires that $(\alpha - \bar{\alpha})/(\zeta - \bar{\zeta})$ be a cyclotomic unit. We use Theorem **??** to reduce this to the requirement that $\gcd(h_q^+, p(p-1)/2) = 1$.

Our proof of Theorem **??** uses three lemmas. The first lemma follows the work of Bremner [**?**] in the case of prime cyclotomic fields.

Lemma 3.1 *Let $\alpha \in \mathbb{Z}[\zeta]$. Then $\mathbb{Z}[\alpha] = \mathbb{Z}[\zeta]$ if and only if*

$$\mathrm{Norm}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\alpha - \sigma_i(\alpha)) = \pm \mathrm{Norm}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta - \zeta^i),$$

for all $1 < i < p^m$, $p \nmid i$.

Proof. An element $\alpha \in \mathbb{Z}[\zeta]$ satisfies $\mathbb{Z}[\alpha] = \mathbb{Z}[\zeta]$ if and only if α and ζ have the same discriminant. This is equivalent to the condition that

$$\mathrm{Norm}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\left(\prod_{\substack{i=2 \\ p \nmid i}}^{p^m} (\alpha - \sigma_i(\alpha))\right) = \mathrm{Norm}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\left(\prod_{\substack{i=2 \\ p \nmid i}}^{p^m} \left(\zeta - \zeta^i\right)\right),$$

which holds if and only if

$$\prod_{\substack{i=2 \\ p \nmid i}}^{p^m} \left(\mathrm{Norm}_{\mathbb{Q}(\zeta)/\mathbb{Q}} \left(\frac{\alpha - \sigma_i(\alpha)}{\zeta - \zeta^i} \right) \right) = 1.$$

Each of the quotients $(\alpha - \sigma_i(\alpha))/(\zeta - \zeta^i)$ is an algebraic integer and so its norm is a rational integer. Thus, the above equation is equivalent to

$$\mathrm{Norm}_{\mathbb{Q}(\zeta)/\mathbb{Q}} \left(\frac{\alpha - \sigma_i(\alpha)}{\zeta - \zeta^i} \right) = \pm 1$$

for all $1 < i < p^m$, $p \nmid i$. The lemma follows. □

Lemma 3.2 *Let t and k be integers such that $0 \leq t < m$ and p does not divide k. Then*

$$\mathrm{Norm}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1 - \zeta^{p^t k}) = p^{p^t}.$$

Proof. Let $\omega = \zeta^{p^t k}$, $p \nmid k$. Then ω is a primitive p^nth root of unity, where $n = m - t$. Thus ω has minimal polynomial

$$\Phi_{p^n}(x) = x^{(p-1)p^{n-1}} + x^{(p-2)p^{n-1}} + \cdots + x^{p^{n-1}} + 1 = \prod_{\substack{i=1 \\ p \nmid i}}^{p^n} (x - \omega^i).$$

This gives that $\mathrm{Norm}_{\mathbb{Q}(\omega)/\mathbb{Q}}(1 - \omega) = \Phi_{p^n}(1) = p$. Since $\deg(\mathbb{Q}(\zeta)/\mathbb{Q}(\omega)) = p^t$, it follows that

$$\mathrm{Norm}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1 - \omega) = \left(\mathrm{Norm}_{\mathbb{Q}(\omega)/\mathbb{Q}}(1 - \omega) \right)^{p^t} = p^{p^t}$$

as claimed. □

Lemma 3.3 *Suppose $\gamma \in \mathbb{Z}[\zeta]$ is a unit, $\mathrm{Norm}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1 - \gamma) = \pm p^i$ for some non-negative even integer i, and $\gamma \notin \mathbb{R}$. Then*

$$\gamma = \frac{\zeta^a - \zeta^b}{\zeta^a - \zeta^{-a}}$$

for some $a, b \in \mathbb{Z}$.

Proof. Any unit of $\mathbb{Z}[\zeta]$ can be written as a root of unity times a real unit (see Washington [**?**]), so there exists $s \in \mathbb{Z}$ and a unit $\mu \in \mathbb{Z}[\zeta + \zeta^{-1}]$ such that $\gamma = \zeta^s \mu$. Since $\gamma \notin \mathbb{R}$, taking the complex conjugate of γ yields $\overline{\gamma} = \zeta^t \gamma \neq \gamma$, where $t = -2s$ and $t \not\equiv 0 \bmod p^m$.

Let $\tau = 1 - \gamma$ and assume $\mathrm{Norm}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\tau) = \pm p^i$, where i is a non-negative even integer. Then $\tau = (\text{unit}) \cdot (1-\zeta)^i$, since $1-\zeta$ is a uniformizing parameter for the prime ideal above p in $\mathbb{Z}[\zeta]$. As above, it follows that $\tau = \zeta^k \varepsilon (1-\zeta)^i$, for some $k \in \mathbb{Z}$ and real unit ε. Since i is even, this gives that $\overline{\tau} = (-1)^i \zeta^{-2k-i} \tau = \zeta^n \tau$, where $n \in \mathbb{Z}$, $n \not\equiv 0 \bmod p^m$.

We have that $\gamma + \tau = 1$ and $\overline{\gamma} + \overline{\tau} = \zeta^t \gamma + \zeta^n \tau = 1$. Solving these two equations for γ gives

$$\gamma = \frac{\zeta^n - 1}{\zeta^n - \zeta^t} = \frac{\zeta^{(n-t)/2} - \zeta^{-(n+t)/2}}{\zeta^{(n-t)/2} - \zeta^{(t-n)/2}} = \frac{\zeta^a - \zeta^b}{\zeta^a - \zeta^{-a}},$$

where $a \not\equiv b \bmod p^m$, and $a \not\equiv 0 \bmod p^m$. □

We are finally ready to prove Theorem **??**.

Proof of Theorem **??**. Assume $\mathbb{Z}[\alpha] = \mathbb{Z}[\zeta]$ and $\gcd(h_q^+, p(p-1)/2) = 1$. First observe that if $\alpha + \overline{\alpha} \in \mathbb{Z}$ then it must be an odd integer. Indeed, suppose $\alpha + \overline{\alpha} = k \in \mathbb{Z}$, and k is even. Then $(\alpha - \overline{\alpha})/2 = \alpha - k/2$ is an element of $\mathbb{Z}[\zeta]$. This is impossible since by Lemmas **??** and **??** it has norm $\pm p/2^{\phi(q)}$, which is not a rational integer.

Now suppose $\alpha + \overline{\alpha} \notin \mathbb{Z}$. We must show that α is equivalent to ζ. In this case, $\alpha + \overline{\alpha}$ is not fixed by $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Thus $\alpha + \overline{\alpha} \neq \sigma_g(\alpha) + \sigma_g(\overline{\alpha})$, where, as usual, σ_g generates $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Thus

$$\gamma = \frac{\alpha - \sigma_g(\alpha)}{\alpha - \overline{\alpha}} \notin \mathbb{R}.$$

The norms of γ and $1-\gamma$ can easily be computed using Lemma **??**, Lemma **??**, and the fact that ζ^i has norm 1 for all $i \in \mathbb{Z}$. Specifically, we have

$$\begin{aligned} \mathrm{Norm}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\gamma) &= \mathrm{Norm}_{\mathbb{Q}(\zeta)/\mathbb{Q}} \left(\frac{\zeta - \zeta^g}{\zeta - \zeta^{-1}} \right) \\ &= \mathrm{Norm}_{\mathbb{Q}(\zeta)/\mathbb{Q}} \left(\frac{1 - \zeta^{g-1}}{1 - \zeta^{-2}} \right) \\ &= 1, \end{aligned}$$

since $g \not\equiv 1 \bmod p$. Also,

$$\mathrm{Norm}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1-\gamma) = \mathrm{Norm}_{\mathbb{Q}(\zeta)/\mathbb{Q}} \left(\frac{\sigma_g(\alpha) - \overline{\alpha}}{\alpha - \overline{\alpha}} \right)$$

$$= \text{Norm}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\left(\frac{\zeta^g - \zeta^{-1}}{\zeta - \zeta^{-1}}\right)$$
$$= \text{Norm}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\left(\frac{1 - \zeta^{g+1}}{1 - \zeta^2}\right).$$

If $p \neq 3$ then $g \not\equiv -1 \bmod p$, so $\text{Norm}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1-\gamma) = 1$ by Lemma **??**. If $p = 3$ then $g \equiv 1 \bmod p$, so $g + 1 = 3^t k$ for some positive integers t and k with $3 \nmid k$. Thus, $\text{Norm}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1-\gamma) = 3^{3^t-1}$ by Lemma **??**. That is, $\text{Norm}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1-\gamma)$ is an even power of 3. Thus Lemma **??** applies in both cases and

$$\gamma = \frac{\alpha - \sigma_g(\alpha)}{\alpha - \overline{\alpha}} = \frac{\zeta^a - \zeta^b}{\zeta^a - \zeta^{-a}}$$

for some $a, b \in \mathbb{Z}$.

We claim that p does not divide a. Theorem **??** follows from this fact and Theorem **??**. Namely, if p does not divide a then there is an integer c with $ac \equiv 1 \bmod p^m$. Let $\sigma_c \in \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ be defined by $\sigma_c(\zeta) = \zeta^c$, and $\alpha' = \sigma_c(\alpha)$. Then

$$\sigma_c(\gamma) = \frac{\alpha' - \sigma_g(\alpha')}{\alpha' - \overline{\alpha}'} = \frac{\zeta - \zeta^{-k}}{\zeta - \zeta^{-1}}, \tag{11}$$

where $k \equiv -bc \bmod p^m$. Thus

$$\frac{\alpha' - \overline{\alpha}'}{\zeta - \overline{\zeta}} = \frac{\alpha' - \sigma_g(\alpha')}{\zeta - \sigma_k(\overline{\zeta})}. \tag{12}$$

Moreover, $(\alpha' - \overline{\alpha}')/(\zeta - \overline{\zeta})$ is a unit by Lemma **??** since $\mathbb{Z}[\alpha] = \mathbb{Z}[\alpha'] = \mathbb{Z}[\zeta]$. It follows from Theorem **??** that $\alpha' = n \pm \zeta$ for some $n \in \mathbb{Z}$. Hence, $\alpha = \sigma_a(\alpha') = n \pm \zeta^a$, and α is equivalent to ζ as claimed in the statement of Theorem **??**.

Thus it remains to prove that if

$$\gamma = \frac{\alpha - \sigma_g(\alpha)}{\alpha - \overline{\alpha}} = \frac{\zeta^a - \zeta^b}{\zeta^a - \zeta^{-a}}$$

then p does not divide a. Suppose that p does divide a. We first show that $\gamma \in \mathbb{Z}[\zeta^p]$. To see this write γ as

$$\gamma = \frac{1 - \zeta^{b-a}}{1 - \zeta^{-2a}}.$$

Since γ is a unit and p divides a, it follows from Lemma **??** that p divides $b-a$. Thus,

$$\gamma = \frac{1-(\zeta^p)^{(b-a)/p}}{1-(\zeta^p)^{-a/p}} \in \mathbb{Z}[\zeta^p].$$

The field $\mathbb{Q}(\zeta^p)$ is fixed by $\tau = (\sigma_g)^{(p-1)p^{m-2}} \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Thus

$$\gamma = \frac{\alpha - \sigma_g(\alpha)}{\alpha - \overline{\alpha}} = \frac{\tau(\alpha) - \tau(\sigma_g(\alpha))}{\tau(\alpha) - \tau(\overline{\alpha})},$$

and so

$$\mu = \frac{\alpha - \sigma_g(\alpha)}{\tau(\alpha) - \tau(\sigma_g(\alpha))} = \frac{\alpha - \overline{\alpha}}{\tau(\alpha) - \tau(\overline{\alpha})} \tag{13}$$

is a unit in $\mathbb{Z}[\zeta + \zeta^{-1}]$. Thus, $\alpha - \overline{\alpha} = \mu(\tau(\alpha) - \tau(\overline{\alpha}))$, and we have

$$\alpha - \mu\tau(\alpha) = \overline{\alpha} - \mu\tau(\overline{\alpha}). \tag{14}$$

Similarly, $\alpha - \sigma_g(\alpha) = \mu(\tau(\alpha) - \tau(\sigma_g(\alpha)))$, and we also have

$$\alpha - \mu\tau(\alpha) = \sigma_g(\alpha) - \mu\tau(\sigma_g(\alpha)). \tag{15}$$

Since $\mu \in \mathbb{R}$, acting on both sides of (**??**) by complex conjugation gives

$$\overline{\alpha} - \mu\tau(\overline{\alpha}) = \sigma_g(\overline{\alpha}) - \mu\tau(\sigma_g(\overline{\alpha})). \tag{16}$$

Notice that the left-hand sides of (**??**) and (**??**) are equal by (**??**). Thus the right-hand sides are equal and we have

$$\sigma_g(\alpha) - \sigma_g(\overline{\alpha}) = \mu\tau(\sigma_g(\alpha)) - \mu\tau(\sigma_g(\overline{\alpha})).$$

Solving this equation for μ gives that

$$\mu = \frac{\sigma_g(\alpha - \overline{\alpha})}{\sigma_g(\tau(\alpha) - \tau(\overline{\alpha}))} = \sigma_g(\mu).$$

Thus μ is fixed by σ_g, and so $\mu \in \mathbb{Z}$. Thus $\mu = \pm 1$ since μ is a unit. We derive a contradiction by considering $\mu = 1$ and $\mu = -1$ separately.

Suppose $\mu = 1$. Then $\alpha - \overline{\alpha} = \tau(\alpha - \overline{\alpha})$ by (**??**). Thus $\alpha - \overline{\alpha}$ is fixed by τ and so $\alpha - \overline{\alpha} \in \mathbb{Z}[\zeta^p]$. Since $\deg(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta^p)) = p$, we have that

$$\mathrm{Norm}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\alpha - \overline{\alpha}) = \Big(\mathrm{Norm}_{\mathbb{Q}(\zeta^p)/\mathbb{Q}}(\alpha - \overline{\alpha})\Big)^p = n^p$$

for some $n \in \mathbb{Z}$. But, from Lemmas **??** and **??**, we know that

$$\mathrm{Norm}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\alpha - \overline{\alpha}) = \pm\mathrm{Norm}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta - \overline{\zeta}) = \pm\mathrm{Norm}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1 - \zeta^2) = \pm p.$$

Thus, $\mathrm{Norm}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\alpha - \overline{\alpha})$ is not a pth power of a rational integer, and we have a contradiction.

It remains to consider $\mu = -1$. In this case (**??**) gives that

$$\alpha + \tau(\alpha) = \sigma_g(\alpha + \tau(\alpha)).$$

Thus $\alpha + \tau(\alpha)$ is fixed by σ_g, and so

$$\alpha + \tau(\alpha) = n, \tag{17}$$

for some $n \in \mathbb{Z}$. Letting τ act on both sides of this equation yields

$$\tau(\alpha) + \tau^2(\alpha) = n. \tag{18}$$

Subtracting equation (**??**) from equation (**??**) gives that $\alpha - \tau^2(\alpha) = 0$, and so α is fixed by $\tau^2 = (\sigma_g)^{2(p-1)p^{m-2}}$. It follows that α is fixed by τ since σ_g has order $(p-1)p^{m-1}$ in $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Therefore, $\alpha \in \mathbb{Q}(\zeta^p)$ and does not generate the ring of integers of $\mathbb{Q}(\zeta)$. We have reached a contradiction. Therefore p does not divide a, as needed to complete the proof of Theorem **??**. □

4 Proof of Conjecture ?? for $q = 25$

In this section we give a short overview of a computation that proves Conjecture **??** for $q = 25$. Using the special properties of the cyclotomic field K we reduce the index form equation corresponding to a power integral basis in K to a unit equation and solve this unit equation by using Baker's method, reduction, and enumeration methods. These algorithms are detailed in Gaál [7].

4.1 Basic data

For $q = 25$ the cyclotomic field K is generated over $\mathbb{Q}$ by the element ζ defined by $f(x) = x^{20} + x^{15} + x^{10} + x^5 + 1$. An integral basis of K is given by $\{1, \zeta, \zeta^2, \ldots, \zeta^{19}\}$, the discriminant of K is $D_K = 5^{35}$. We denote a set of fundamental units of K by $\{\mu_1, \ldots, \mu_9\}$. This data can be computed e.g. by KASH [**?**], which gives that the coefficients of our set of fundamental units with respect to the integral basis $\{1, \zeta, \zeta^2, \ldots, \zeta^{19}\}$ are the following:

$$\begin{aligned}
\mu_1 &= (-1,0,0,0,0,-1,0,0,0,0,-1,0,0,0,0,0,0,0,0,0)\\
\mu_2 &= (0,0,-1,0,0,1,0,-1,0,0,0,0,-1,0,0,0,0,-1,0,0)\\
\mu_3 &= (1,0,-1,0,0,0,0,-1,0,0,0,0,-1,0,0,0,0,-1,0,0)
\end{aligned}$$

$$
\begin{aligned}
\mu_4 &= (1,0,0,-1,0,0,0,0,-1,0,0,0,0,-1,0,0,0,0,-1,0)\\
\mu_5 &= (1,-1,0,0,0,0,-1,0,0,0,0,-1,0,0,0,0,-1,0,0,0)\\
\mu_6 &= (1,0,0,0,-1,0,0,0,0,-1,0,0,0,0,-1,0,0,0,0,-1)\\
\mu_7 &= (0,0,0,0,0,-1,0,0,0,0,0,0,0,0,-1,0,0,0,0,0)\\
\mu_8 &= (-1,0,0,0,1,-1,0,1,-1,1,-1,-1,1,-1,0,0,-1,1,0,0)\\
\mu_9 &= (0,-1,0,0,0,1,-1,1,-1,0,0,-1,1,-1,1,0,0,0,-1,0)
\end{aligned}
$$

As denoted in Section 2, the automorphisms of K are given by $\sigma_i : \zeta \mapsto \zeta^i$ with $5 \nmid i$, $1 \le i \le 25$. We have $D_K = \prod \left(\zeta^i - \zeta^j\right)^2$, where the product is taken for $1 \le i < j \le 25$ with $5 \nmid ij$.

4.2 From power integral bases to unit equations

Assume that the integer $\alpha = x_0 + x_1\zeta + x_2\zeta^2 + \ldots + x_{19}\zeta^{19} \in K$ generates a power integral basis in K. The conjugates of α are $\sigma_i(\alpha) = x_0 + x_1\zeta^i + x_2\zeta^{2i} + \ldots + x_{19}\zeta^{19i}$ for the above indices i. The elements $\{1, \alpha, \alpha^2, \ldots, \alpha^{19}\}$ form an integral basis if and only if $I(\alpha) = 1$, where $I(\alpha)$ denotes the index of α in $\mathcal{O}_K$. Thus we have

$$
I(\alpha) = \frac{\prod |\sigma_i(\alpha) - \sigma_j(\alpha)|}{\sqrt{D_K}} = \prod |\eta_{ij}| = 1, \tag{19}
$$

where the products are taken for $1 \le i < j \le 25$ with $5 \nmid ij$, and

$$
\eta_{ij} = \frac{\sigma_i(\alpha) - \sigma_j(\alpha)}{\zeta^i - \zeta^j} = x_1 + x_2\frac{\zeta^{2i} - \zeta^{2j}}{\zeta^i - \zeta^j} + \ldots + x_{19}\frac{\zeta^{19i} - \zeta^{19j}}{\zeta^i - \zeta^j} \tag{20}
$$

are units in K by Lemma **??**.

Let $a_1, \ldots, a_9$ be integers with

$$
\eta_{12} = \pm\xi_{12}\, \mu_1^{a_1} \cdots \mu_9^{a_9},
$$

where ξ_{12} is a root of unity in K. We are going to determine $a_1, \ldots, a_9$.

Note that $x_1, \ldots, x_{19}$ can be easily calculated from $a_1, \ldots, a_9$. Indeed, for a given tuple $(a_1, \ldots, a_9)$ we consider η_{12} as a linear form in the variables $x_1, \ldots, x_{19}$ by (**??**). Taking conjugates of η_{12} we obtain a system of linear equations in $x_1, \ldots, x_{19}$. This system can be uniquely solved for $x_1, \ldots, x_{19}$ (cf. Section 4.1 of [7]).

To calculate $a_1, \ldots, a_9$ we use the identity

$$
\frac{\zeta^2 - \zeta^4}{\zeta^2 - \zeta} \cdot \frac{\eta_{24}}{\eta_{12}} + \frac{\zeta^4 - \zeta}{\zeta^2 - \zeta} \cdot \frac{\eta_{41}}{\eta_{12}} \;=\; 1, \tag{21}
$$

which is immediate from the definition of η_{ij} in (**??**). We have

$$\frac{\zeta^2-\zeta^4}{\zeta^2-\zeta}=\zeta^2\cdot\mu_6.$$

Further, in the numerator,

$$\eta_{24}=\sigma_2(\eta_{12})=\pm\sigma_2(\xi_{12})\,(\sigma_2(\mu_1))^{a_1}\cdots(\sigma_2(\mu_9))^{a_9}.$$

We can express each $\sigma_2(\mu_k)$ as a power product of $\mu_1,\dots,\mu_9$ (up to a root of unity). This gives

$$\frac{\zeta^2-\zeta^4}{\zeta^2-\zeta}\cdot\frac{\eta_{24}}{\eta_{12}}=\xi_1\cdot\mu_1^{A_1}\cdots\mu_9^{A_9},$$

where ξ_1 is a root of unity and

$$\begin{pmatrix}A_1\\A_2\\A_3\\A_4\\A_5\\A_6\\A_7\\A_8\\A_9\end{pmatrix}=\begin{pmatrix}-2&0&1&0&0&0&0&0&0\\0&-1&0&0&1&0&0&0&0\\0&0&-1&0&0&0&0&0&1\\0&0&0&-1&0&1&0&0&0\\0&0&-1&1&-1&0&0&0&0\\0&0&-1&0&0&-1&0&0&0\\0&1&0&0&0&0&-1&1&-1\\0&0&-1&0&0&0&-1&-2&0\\0&0&-1&0&0&0&0&-1&0\end{pmatrix}\cdot\begin{pmatrix}a_1\\a_2\\a_3\\a_4\\a_5\\a_6\\a_7\\a_8\\a_9\end{pmatrix}+\begin{pmatrix}0\\0\\0\\0\\0\\1\\0\\0\\0\end{pmatrix}\quad.\tag{22}$$

The above matrix is invertible, so we can calculate $a_1,\dots,a_9$ from $A_1,\dots,A_9$.

Further, there are integers $B_1,\dots,B_9$ such that

$$\frac{\zeta^4-\zeta}{\zeta^2-\zeta}\cdot\frac{\eta_{41}}{\eta_{12}}=\xi_2\cdot\mu_1^{B_1}\cdots\mu_9^{B_9},$$

where ξ_2 is a root of unity. Hence we can write equation (**??**) in the form

$$\xi_1\cdot\mu_1^{A_1}\cdots\mu_9^{A_9}+\xi_2\cdot\mu_1^{B_1}\cdots\mu_9^{B_9}=1.\tag{23}$$

The unit equation (**??**) has the big advantage that its terms are completely symmetric.

In the following subsections we only give a sketch of the algorithms used to compute $A_1,\dots,A_9$ since they are similar to those we have used at other times, cf. Gaál [7].

4.3 Baker's method

Set $B=\max|B_k|$ and $A=\max|A_k|$. If $B\geq A$ (the other case should be considered similarly), then (if A is large enough) by using standard tools it follows from equation (**??**) that

$$|A_1\log|\sigma_k(\mu_1)|+\ldots+A_9\log|\sigma_k(\mu_9)||<c_1\exp(-c_2A)$$

for some conjugate k and positive constants c_1, c_2. Using Baker type estimates it can be shown that the above linear form can be estimated from below by $\exp(-C \log A)$, where C is a (large) positive constant. Comparing the lower and upper estimates we can derive an upper bound for A (see e.g. Section 7.1 of [7]), which was 10^{64} in our example.

4.4 Reduction

Using the above inequality and Lemma 2.2.2 of [7] this upper bound for A can be reduced. Note that this procedure involves LLL reduction with high precision numbers. To illustrate our computation we give some data on the reduction steps:

Step	$A \leq$	Digits	New Bound	CPU Time
$I.$	10^{64}	1500	60556	107 min
$II.$	60556	200	6790	4 min
$III.$	6790	200	5230	3 min
$IV.$	5230	200	4931	3 min

Finally we obtain the upper bound 4931 for A. Recall that this bound for A was derived under the assumption $A \leq B$. Equation (23) implies

$$|B_1 \log|\sigma_k(\mu_1)| + \ldots + B_9 \log|\sigma_k(\mu_9)|| = |\log|1 - \sigma_k(\xi_1)\sigma_k(\mu_1)^{A_1} \ldots \sigma_k(\mu_9)^{A_9}||$$

for all conjugates k. In view of $A \leq 4931$, the right-hand side can be estimated from above. We consider this system as a system of linear equations. Using nine suitable conjugates k, such that the matrix on the left side of the system is invertible, we calculate the inverse of this matrix and use the upper estimate for the terms on the right side to obtain the bound $B \leq 91351$.

4.5 Enumeration

In equation (**??**) we put $\varepsilon_1 = \xi_1 \cdot \mu_1^{A_1} \cdots \mu_9^{A_9}$, $\varepsilon_2 = \xi_2 \cdot \mu_1^{B_1} \cdots \mu_9^{B_9}$, then both ε_1 and ε_2 are units in K and equation (**??**) can be written in the form

$$\varepsilon_1 + \varepsilon_2 = 1. \tag{24}$$

(Such units are called *exceptional units*.) The upper bound of 91351 for A and B implies that all conjugates of $\varepsilon_1, \varepsilon_2, 1/\varepsilon_1, 1/\varepsilon_2$ are in absolute value less than $S_0 = 10^{733559}$. It is easily seen that if $\varepsilon = \varepsilon_1$ is a solution of (**??**) then so are all elements of the *orbit* of ε,

$$\Omega(\varepsilon) = \left\{\varepsilon, 1-\varepsilon, \frac{1}{\varepsilon}, \frac{1}{1-\varepsilon}, \frac{\varepsilon-1}{\varepsilon}, \frac{\varepsilon}{\varepsilon-1}\right\},$$

as well as all conjugates of elements of $\Omega(\varepsilon)$.

The following lemma can be proved by standard elementary means, using the arguments of Wildanger [**?**].

Lemma 4.1 *Let $s < S$ be positive constants and let ε be a solution of equation (**??**) with*

$$\frac{1}{S} < |\sigma_k(\varepsilon)| < S \tag{25}$$

for all conjugates k. Then either

$$\frac{1}{s} < |\sigma_k(\varepsilon)| < s$$

for all conjugates k, or there is an element $\eta \in \Omega(\varepsilon)$ and a conjugate $\eta_0 = \sigma_j(\eta)$ such that

$$|\eta_0 - 1| < \frac{1}{s}. \tag{26}$$

In view of the remark before the lemma, η_0 is a solution of (**??**). Using standard means we can see that the exponent vector $(z_1, \ldots, z_9)$, which corresponds to the solution $\eta_0 = \xi \cdot \mu_1^{z_1} \cdots \mu_9^{z_9}$ (ξ a root of unity) of (**??**) satisfying (**??**) for all conjugates and (**??**) for a certain conjugate, lies in an ellipsoid that can be enumerated by using the ideas of Wildanger [**?**]. Then, at the price of enumerating the integer points in some ellipsoids, we can replace S in (**??**) by s. The above lemma made the enumeration process more efficient.

The enumeration involving all possible conjugates j was performed according to the following table. The last column indicates the number of exponent vectors found. The last ellipsoid (in the last line) corresponds to those ε satisfying (**??**) with $S = 20$.

S	s	Digits	CPU Time	#Tuples
10^{733559}	10^{100}	300	2 min	1
10^{100}	10^{20}	300	0.2 min	7
10^{20}	10^{15}	70	0.2 min	1
10^{15}	10^{12}	60	0.5 min	202
10^{12}	10^{10}	50	12 min	3036
10^{10}	10^{9}	50	35 min	6676
10^{9}	10^{8}	50	150 min	27816
10^{8}	10^{7}	50	276 min	101460
10^{7}	10^{6}	50	1775 min	329404
10^{6}	$5 \cdot 10^{5}$	50	1072 min	192409
$5 \cdot 10^{5}$	$3 \cdot 10^{5}$	50	1150 min	212100
$3 \cdot 10^{5}$	10^{5}	50	2203 min	455978
10^{5}	$5 \cdot 10^{4}$	50	1497 min	449108
$5 \cdot 10^{4}$	$3 \cdot 10^{4}$	50	2362 min	460663
30000	11000	50	4260 min	839334
11000	7000	50	2900 min	579944
7000	2500	50	4648 min	1059429
2500	1000	50	5100 min	998951
1000	300	50	5910 min	1203260
300	200	50	1920 min	404138
200	80	50	2285 min	548199
80	50	50	784 min	198971
50	20	50	769 min	202613
20		50	5850 min	1269078

The enumeration took about 31 days, which was very surprising since the resolution of some similar unit equations with higher unit ranks were usually much faster. This could be due to the symmetry properties of the cyclotomic field.

In parallel to the enumeration we made a modular test (sieve) to select those exponent tuples that correspond to solutions of equation (**??**) (which of course made the enumeration process much longer but spared a further test). Out of the approximately $9.5 \cdot 10^6$ enumerated tuples we found about 40000 "good" tuples. For each of these tuples $(z_1, \ldots, z_9)$ and all possible roots of unity ξ (according to the notes after Lemma **??**) we had to consider all orbit elements of all conjugates of $\xi\mu_1^{z_1} \cdots \mu_9^{z_9}$, which took about a further 30 days of CPU time. For all these possible solutions $\varepsilon_1 = \xi_1 \cdot \mu_1^{A_1} \cdots \mu_9^{A_9}$ of the unit equation we calculated the corresponding exponent vector $(a_1, \ldots, a_9)$ from (**??**) and constructed the possible generators α of power integral bases. Before checking their indices we used the criterion for $\alpha + \overline{\alpha}$ given in Theorem **??** to eliminate almost all possible elements. The only elements α of index one that satisfied $\alpha + \overline{\alpha} = 1$ were the Galois conjugates of $1/(1+\zeta)$. Therefore, Conjecture **??** holds for $q = 25$.

All computations were performed in Maple on a PC with 900 Mhz under

Linux.

References

[1] A. Bremner, On power bases in cyclotomic number fields, *J. Number Theory* **28** (1988), 288–298.

[2] J. Buhler, R. Crandall, R. Ernvall, T. Metsänkylä, and A. Shokrollahi, Irregular primes and cyclotomic invariants to twelve million, *J. Symb. Comp.* **31** (2001), 89–96.

[3] J. Buhler, C. Pomerance, and L. Robertson, Heuristics for class numbers of prime-power real cyclotomic fields, *High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams* (Banff, AB, 2003), Fields Inst. Commun. **41**, 149-157, Amer. Math. Soc., Providence, RI, 2004.

[4] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner and K. Wildanger, KANT V4, *J.Symbolic Comput.* **24** (1997), 267–283.

[5] R. Dedekind, Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen, *Abh. Kgl. Ges. Wiss. Göttingen* **23** (1878), 1–23.

[6] F. van der Linden, Class number computations of real abelian number fields. *Math. Comp.* **39** (1982), 693-707.

[7] I. Gaál, *Diophantine equations and power integral bases. New computational methods*, Birkhäuser, Boston, 2002.

[8] I. Gaál and M. Pohst, On the resolution of index form equations in sextic fields with an imaginary quadratic subfield, *J. Symbolic Comput.*, **22** (1996), 425–434.

[9] K. Győry, Discriminant form and index form equations, *Algebraic Number Theory and Diophantine Analysis*, de Gruyter, 2000, 191–214.

[10] K. Győry, Sur les polynômes à coefficients entiers et de discriminant donné, III, *Publ. Math. Debrecen* **23** (1976), 141–165.

[11] L. Robertson, Power bases for cyclotomic integer rings, *J. Number Theory* **69** (1998), 98–118.

[12] L. Robertson, Power bases for 2-power cyclotomic fields, *J. Number Theory* **88** (2001), 196–209.

[13] R. Schoof, Class numbers of real cyclotomic fields of prime conductor, *Math. Comp.* **72** (2003), 913–937.

[14] L. Washington, *Introduction to Cyclotomic Fields,* 2nd ed., Springer–Verlag, New York, 1997.

[15] K. Wildanger, Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern, *J. Number Theory* **82** (2000), 188–224.